超楕円曲線とmod 2ガロア表現について (代数的整数論とその周辺)

AUTHOR(S):

橋本, 喜一朗

CITATION:

橋本, 喜一朗. 超楕円曲線とmod 2ガロア表現について (代数的整数論とその周辺). 数理解析研究所講究録 2005, 1451: 285-294

ISSUE DATE:

2005-10

URL:

http://hdl.handle.net/2433/47747

数理解析研究所講究録 1451 巻 2005 年 285-294

超楕円曲線と mod 2 ガロア表現について

早稲田大学・理工学部　橋本 喜一朗 (Kiichiro Hashimoto)
Department of Mathematical Sciences,
Waseda University

0. はじめに

k を標数が 0 の体, $\overline{k}$ をその代数閉包, n を $n>4$ なる正整数とする. k 係数のモニックな n 次分離的多項式 $f(X)\in k[X]$ に対して, その n 個の零点に一つの順序を指定して $a_1,\ldots,a_n\in\overline{k}$ とする. このとき $f(X)$ の k 上のガロア群は, これらが充たす k 上のあらゆる代数関係式を保つ $a_1,\ldots,a_n$ の置換の全体からなる群である: すなわち, 点 $(a_1,..,a_n)\in\mathbb{A}^n(\overline{k})$ を零点とする k 上の n 変数多項式からなるイデアルを $I_f:=\{F\in k[X_1,..,X_n]\mid F(a_1,..,a_n)=0\}$ とするとき

$$\mathrm{Gal}(f/k) \;=\; \{\sigma\in\mathcal{S}_n\mid \sigma(I_f)\subseteq I_f\}.$$

ここで $a_1,\ldots,a_n$ の置換を添え字の置換 $\sigma\in\mathcal{S}_n$ と同一視する ($\mathcal{S}_n$ は n 次対称群, 以下同様). 言うまでもなく $f(X)$ の k 上の (最小) 分解体は $\mathrm{Spl}(f/k)=k(a_1,\ldots,a_n)$ で, $\mathrm{Gal}(f/k)$ は拡大 $k(a_1,\ldots,a_n)/k$ のガロア群と一致する.

$f(X)\in k[X]$ に対して, 次式を定義方程式とする k 上の超楕円曲線 X_f を対応させる:

$$X_f:\quad y^2 \;=\; f(x) \tag{1}$$

本稿の目的は, この対応 $f\mapsto X_f$ を通して $\mathrm{Gal}(f/k)$ を眺めること, または逆に $\mathrm{Gal}(f/k)$ の情報が X_f にどの程度反映されるかについて簡単な考察を行うことである. 特に, この対応から自然に発生する二つの素朴な問題 (以下の**問題 1, 問題 2**) について考察する.

この対応は一見安直に見えるが, 実際には非常に重要で, 既に多くの研究がある: 森氏の研究 [7], Mumford の本 [9] の末尾の梅村氏による Appendix. 最近では Zarhin の一連の研究 ([11]) など. 特に, 問題 1 についての結果は, 梅村氏の論稿 ([9]) 中に述べられている事実を W.Meyer [5] に沿って整理したもので, 新しい結果ではないが, 本稿のように mod 2 ガロア表現と $\mathbb{F}_2$ 上の幾何の関係をキチンと記述しておくことは無意味ではないであろうと思う.

1. 問題 1 について

超楕円曲線 X_f の種数を g とすると n が奇数 (resp. 偶数) のとき $n=2g+1$ (resp. $n=2g+2$) となる. 以下 n,g はこの関係を保つものとする. X_f は $X_f\ni(x,y)\mapsto x\in\mathbb{P}^1$ により射影直線 $\mathbb{P}^1$ の 2 重被覆であり, その分岐点の集合は

$$B_f \;=\; \begin{cases} \{P_i=(a_i,0)\mid 1\le i\le n\} & (n=2g+2)\\ \{P_i=(a_i,0)\mid 1\le i\le n\}\cup\{P_\infty=(\infty,\infty)\} & (n=2g+1)\end{cases} \tag{2}$$

となる. B_f は X_f の Weierstrass 点の全体と一致する. このとき $\mathrm{Gal}(f/k)$ は B_f への自然に作用し, したがって $\mathcal{S}_{2g+2}$ に埋め込まれる (置換表現). 他方, この表現は X_f のヤコビ多様体の 2 等分点におけるガロア表現とみなせる. 一般 n 次方程式のガロア群は n 次対称群であるから, このようにして $\mathrm{Gal}(f/k)\cong\mathcal{S}_{2g+2}$ $(n=2g+2)$ が $\mathrm{GSp}(2g,\mathbb{F}_2)=\mathrm{Sp}(2g,\mathbb{F}_2)$ に埋め込まれることが判る. そこで次の問題が生じる.

• **問題 1** $\mathcal{S}_{2g+2}$ を $\mathrm{Sp}(2g,\mathbb{F}_2)$ の部分群として実現する初等的で自然な (幾何学的) 記述を与えよ.

注意 1 良く知られているように 同型 $\mathrm{Sp}(4,\mathbb{F}_2)\cong\mathcal{S}_6$ $(g=2)$ が成立する. しかし $g=3,4$ では $\mathcal{S}_8,\mathcal{S}_{10}$ は各々$\mathrm{Sp}(6,\mathbb{F}_2)$, $\mathrm{Sp}(8,\mathbb{F}_2)$ の極大部分群で指数は各々 36, 13056 となる. また有限体 $\mathbb{F}_q$ 上のシンプレクティック群 $\mathrm{Sp}(2g,\mathbb{F}_q)$ の位数は

$$|\mathrm{Sp}(2g,\mathbb{F}_q)| \;=\; q^{g^2}\prod_{i=1}^{g}(q^{2i}-1)$$

でこの値は $g>1$ のとき $(2g+2)!$ の倍数になるが, $\ell\neq 2$ の場合一般には $\mathcal{S}_{2g+2}$ は $\mathrm{Sp}(2g,\mathbb{F}_\ell)$ の部分群とならない.

2. J_f の 2 等分点について (復習)

X_f のヤコビ多様体 (主偏極アーベル曲面) を J_f とする. 各素数 ℓ に対して J_f の ℓ 冪等分点のなす ℓ-可除群 $J_f[\ell^\infty]:=\{P\in J_f\mid \exists n,\ell^nP=O\}\cong\left(\mathbb{Q}_\ell/\mathbb{Z}_\ell\right)^{2g}$ への自然な $\mathrm{G}_k:=\mathrm{Gal}(\overline{k}/k)$ の作用は ℓ-進ガロア表現

$$\rho_{f,\ell}\;:\;\mathrm{G}_k\;\longrightarrow\;\mathrm{GSp}(2g,\mathbb{Z}_\ell) \tag{3}$$

を導く. 特にこの表現を mod ℓ すると ℓ 等分点 $J_f[\ell]$ での (mod ℓ) ガロア表現

$$\overline{\rho}_{f,\ell}\;:\;\mathrm{G}_k\;\longrightarrow\;\mathrm{GSp}(2g,\mathbb{F}_\ell) \tag{4}$$

を得る. ここで $\ell=2$ とすると $\overline{\rho}_{f,2}$ (の像) は, 以下のように $\mathrm{Gal}(f/k)$ と密接に関連する.

まず J_f は $\mathrm{Pic}^0(X_f):=\mathrm{Div}^0(X_f)/P(X_f)$ と同一視される. ここで

$$\mathrm{Div}^0(X_f)(\overline{k})\;:=\;\{\sum_{i=1}^{n}m_iQ_i\mid n\geq 0,\ Q_i\in X_f(\overline{k}),\ \sum_{i=1}^{n}m_i=0\}$$

は X_f の次数 0 の因子の群,

$$P(X_f)(\overline{k})\;:=\;\{\mathrm{div}(f)\mid f\in\overline{k}(X_f)^\times\}$$

は X_f の主因子の群である. さて代数曲線を扱った大概の書物では基礎体は代数閉体であるから $n=2g+1$ (奇数) の場合のみが扱われている. この場合, 典型的な主因子としては

$$\begin{cases} \mathrm{div}(x-a_i)=2(P_i-P_\infty), & (1\le i\le 2g+1) \\ \mathrm{div}(y)=(P_1+\cdots+P_{2g+1})-(2g+1)P_\infty \end{cases}$$

がある. この最初の式から

$$e_i \;:=\; [P_i-P_\infty] \quad \in \mathrm{Pic}^0 \qquad (1\le i\le 2g+1) \tag{5}$$

は位数が 2, すなわち $J_f[2]$ の元であることが判る. 第二の式からは $J_f[2]$ における関係式

$$e_1+\cdots+e_{2g+1} \;=\; 0$$

が出る. ここで $\{1,2,\ldots,2g+1\}$ の各部分集合 S に対して

$$e_S \;:=\; \sum_{i\in S} e_i$$

とおくと (6) から $e_S=e_{\overline{S}}$ ($\overline{S}$ は S の補集合) となる. 実は更に以下のことが知られている (Mumford [9] 参照).

命題 1 *$n=2g+1$ (奇数) のとき 加法群 $J_f[2]$ は以下のように記述される:*

$$\begin{aligned} J_f[2] &= \{e_S \mid |S|\equiv 0 \mod 2\}, \\ e_S+e_T &= e_{S\circ T}, \qquad S\circ T := S\cup T - S\cap T. \end{aligned}$$

これと J_f が k 上定義されたアーベル多様体であることから, $k(J_f[2])=k(a_1,..,a_n)=f$ の k 上の最小分解体となることが判る. このことは $n=2g+2$ (偶数) の場合も成り立つ. すなわち, $n=2g+2$ (偶数) の場合は $f(X)$ の零点に $k(a_{2g+2})$ 上の分数一次変換 $x\mapsto 1/(x-a_{2g+2})$ を一斉に施して, $(a_1,a_2,\ldots,a_{2g+2})$ を $(a_1{}',a_2',\ldots,a'_{2g+1},\infty)$ に移すことが出来る. このとき X_f は曲線 $y^2=(x-a_1{}')\ldots(x-a'_{2g+1})$ と $k(a_{2g+2})$ 上同型であるから $n=2g+1$ (奇数) の場合の議論に帰着する.

2. Asyzygetic system

$V:=\mathbb{F}_2^{2g}$ とし V に標準交代形式

$$F(\vec{x},\vec{y}) \;=\; \sum_{i=1}^{g} x_iy_{i+g}-y_ix_{i+g}$$

を入れる. $\mathrm{GSp}(2g,\mathbb{F}_2)=\mathrm{Sp}(2g,\mathbb{F}_2)=\mathrm{Aut}(V,F)$ である.

定義 1 $(\vec{x}_{i,j}) \in V^{(2g+2)^2}$ $(1 \leq i,j \leq 2g+2)$ が以下の 2 条件を満たすとき, *Asyzygetic system (A-system)* であるという.

$$\begin{aligned} (i) \quad \vec{x}_{i,j} + \vec{x}_{j,k} + \vec{x}_{k,i} &= \vec{0} \quad (\forall\, i,j,k) \\ (ii) \quad F(\vec{x}_{i,j}, \vec{x}_{i,k}) &= 1 \quad (\forall\, i,j,k : \text{distinct}). \end{aligned}$$

定義から直ちに判るように $\vec{x}_{i,i} = \vec{0}$ $(\forall\, i)$, $\vec{x}_{i,j} = \vec{x}_{j,i}$ $(\forall\, i,j)$. また (i) で $k = 2g+2$ として

$$\vec{x}_{i,j} = \vec{x}_{i,2g+2} + \vec{x}_{j,2g+2} \quad (\forall\, i,j)$$

を得る. 以下 $\vec{x}_i := \vec{x}_{i,2g+2}$ と記すとき $\{\vec{x}_1, \ldots, \vec{x}_{2g}\}$ の Gramm 行列は

$$G := (F(\vec{x}_i, \vec{x}_j)) = \begin{pmatrix} 0 & 1 & \ldots & 1 \\ 1 & 0 & \ldots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 0 \end{pmatrix}$$

となるので $G^2 = I_{2g}$. 従って $\{\vec{x}_1, \ldots, \vec{x}_{2g}\}$ は一次独立で V の基底をなす. 次に (ii) から $F(\vec{x}_1 + \ldots + \vec{x}_{2g+1}, \vec{x}_i) = 2g = 0$ $(i = 1, .., 2g)$. これと F の非退化性より $\vec{x}_1 + \ldots + \vec{x}_{2g+1} = \vec{0}$ すなわち

$$\vec{x}_{2g+1} = \vec{x}_1 + \ldots + \vec{x}_{2g}.$$

以上は A-system の定義から出る性質の一部であるが, これらを逆に辿って (V,F) に対して A-system の存在が示される.

命題 2 $\mathbb{F}_2$ 上の (非退化) 交代形式付きの $2g$ 次元ベクトル空間 (V,F) に対して A-system が存在する.

証明. (V,F) のシンプレクティック基底を $\{\vec{a}_1, \vec{b}_1, \ldots, \vec{a}_g, \vec{b}_g, \}$ とする:

$$F(\vec{a}_i, \vec{a}_j) = F(\vec{b}_i, \vec{b}_j) = 0, \quad F(\vec{a}_i, \vec{b}_j) = \delta_{i,j} \qquad (\forall\, i,j).$$

このとき $\vec{x}_1, \ldots, \vec{x}_{2g+2} \in V$ を以下の如く定める:

$$\begin{aligned} \vec{x}_1 &= \vec{a}_1, \\ \vec{x}_2 &= \vec{b}_1, \\ &\cdots \\ \vec{x}_{2i+1} &= (\vec{a}_1 + \vec{b}_1 + \ldots + \vec{a}_i + \vec{b}_i) + \vec{a}_{i+1} \qquad (0 \leq i \leq g-1) \\ \vec{x}_{2i+2} &= (\vec{a}_1 + \vec{b}_1 + \ldots + \vec{a}_i + \vec{b}_i) + \vec{b}_{i+1} \qquad (0 \leq i \leq g-1) \\ \vec{x}_{2g+1} &= \vec{x}_1 + \ldots + \vec{x}_{2g} = \vec{a}_1 + \vec{b}_1 + \ldots + \vec{a}_g + \vec{b}_g, \\ \vec{x}_{2g+2} &= \vec{0}. \end{aligned}$$

このとき

$$\begin{aligned}\vec{x}_{i,2g+2} &= \vec{x}_i \quad (1 \le i \le 2g+2)\\ \vec{x}_{i,j} &= \vec{x}_{i,2g+2} + \vec{x}_{j,2g+2} \quad (1 \le i,j \le 2g+2)\end{aligned}$$

と置けば $(\vec{x}_{i,j}) \in V^{(2g+2)^2}$ は A-system となる. □

さて $\mathcal{X} = (\vec{x}_{i,j})$ を A-system とする. このとき $\sigma \in \mathcal{S}_{2g+2}c$ に対して

$$\sigma(\mathcal{X}) := (\vec{x}'_{i,j}), \quad \vec{x}'_{i,j} = \vec{x}_{\sigma(i),\sigma(j)}$$

とおけば明らかに $\sigma(\mathcal{X})$ も A-system をなすが, 上の議論から $\{\vec{x}_1, \ldots, \vec{x}_{2g}\}$ $(\vec{x}_i := \vec{x}_{i,2g+2})$ は V の基底であるから,

$$\overline{\sigma} : \vec{x}_{i,j} \mapsto \vec{x}'_{i,j}$$

は (V,F) の自己同型を定める. かくして次の定理が成立する:

定理 1 (V,F) を $\mathbb{F}_2$ 上の (非退化) 交代形式付きの $2g$ 次元空間, $\mathcal{X}$ をその A-system とするとき

$$\begin{aligned}h : \mathcal{S}_{2g+2} &\rightarrowtail \mathrm{Sp}(2g,\mathbb{F}_2) = \mathrm{Aut}(V,F), \qquad \sigma \mapsto \overline{\sigma}\\ \overline{\sigma} : \vec{x}'_{i,j} &\mapsto \vec{x}'_{i,j} = \vec{x}_{\sigma(i),\sigma(j)}\end{aligned}$$

は 対称群 $\mathcal{S}_{2g+2}$ の $\mathrm{Sp}(2g,\mathbb{F}_2)$ への自然な埋め込みを与える. □

$n = 2g+2$ (偶数) のとき X_f の主因子の典型的な例は

$$\begin{aligned}\mathrm{div}(x-a_i) &= 2P_i - (Q_\infty + Q'_\infty) \qquad (1 \le i \le 2g+2)\\ \mathrm{div}\left(\frac{x-a_i}{x-a_j}\right) &= 2(P_i - P_j) \qquad (1 \le i,j \le 2g+2)\end{aligned} \tag{6}$$

である. ここで, Q_∞, Q'_∞ は $x = \infty \in \mathbb{P}^1$ の上にある X_f の点. 従ってこの第 2 の式から

$$e_{i,j} := [P_i - P_\infty] \quad \in \mathrm{Pic}^0 \qquad (1 \le i,j \le 2g+2) \tag{7}$$

は位数が 2, すなわち $J_f[2]$ の元であることが判る. さて $V := J_f[2]$ は $\mathbb{F}_2$ 上の $2g$ 次元ベクトル空間とみなされるが, 主偏極による同一視 $J_f \cong J_f{}^\vee$ から定まる pairing

$$F : J_f[2] \times J_f[2] \longrightarrow \mu_2 \cong \mathbb{F}_2 \tag{8}$$

はこの上の (非退化) 交代形式を定める.

定理 2 (V,F) を $V := J_f[2]$ および *pairing* (8) による交代形式とするとき $(e_{i,j})_{1\leq i,j\leq 2g+2}$ は *A-system* をなす.

証明. 条件 (i) は自明. (ii) は Mumford [9] Prop.6.3 から出る. □

3. 写像類群と Hyperelliptic involution の中心化群

一般に特殊な例外を除いて, 十分に「一般的」な代数曲線 X/k に対して, そのヤコビ多様体 $J(X)$ が非自明な自己準同型をもたない (i.e., $\mathrm{End}_{\overline{k}}(J(X))\cong\mathbb{Z}$) とき, ℓ-進ガロア表現 $\rho_{f,\ell}$ の像は $\mathrm{GSp}(2g,\mathbb{Z}_\ell)$ 全体であると信じられているようである. が, 上述のように, 超楕円曲線 X_f/k に対する mod 2 ガロア表現 $\overline{\rho}_{f,2}$ の像は $\mathrm{GSp}(2g,\mathbb{F}_2)$ 全体にはならず, 高々 S_{2g+2} 内に留まる. このことは, ヤコビ多様体 $J(X)$ の自己準同型環のみを用いてではなく, 以下のように X の基本群に付随する外ガロア表現の枠組みから自然に説明ができる. 以下では k は $\mathbb{C}$ の部分体とする.

$$\pi_1(X(\mathbb{C}),*) \;=\; \left\langle \alpha_1,..,\alpha_g,\beta_1,..,\beta_g \mid \prod_{i=1}^{g}[\alpha_i,\beta_i]=1 \right\rangle \tag{9}$$

を X の基本群とする. そのアーベル化

$$\psi:\pi_1(X(\mathbb{C}),*)\longrightarrow \pi_1(X(\mathbb{C}),*)^{ab}=\mathrm{H}_1(X(\mathbb{C}),\mathbb{Z})=\bigoplus_{i=1}^{g}(\mathbb{Z}a_i\oplus\mathbb{Z}b_i)$$

は 1 次元ホモロジー群で, $\{a_i,b_i\quad(1\leq i\leq g)\}$ は標準交差形式に関するシンプレクティック基底をなす. 他方

$$\Gamma_g \;=\; \mathrm{Out}^+(\pi_1(X(\mathbb{C}),*)) \;=\; \mathrm{Diff}^+(X(\mathbb{C}))/(\text{isotopy}) \tag{10}$$

を 種数 g の写像類群 (Teichmüller モジュラー群) とすると Γ_g の自然な $\mathrm{H}_1(X(\mathbb{C}),\mathbb{Z})$ への作用から標準的準同型

$$\psi_*:\Gamma_g \;\longrightarrow\; \mathrm{Aut}(\mathrm{H}_1(X(\mathbb{C}),\mathbb{Z})) \;=\; \mathrm{Sp}(2g,\mathbb{Z}) \tag{11}$$

が定まる. ここで

定義 2 $i\in\Gamma_g$ は $i^2=1$, かつ $\psi_*(i)=-I_{2g}\in\mathrm{Sp}(2g,\mathbb{Z})$ をみたすとき超楕円対合 *(hyperelliptic involution)* と呼ばれる. また $i\in\Gamma_g$ をそのような元の一つとするとき

$$H_g(i) \;:=\; \{h\in\Gamma_g \mid hoi=ioh\} \tag{12}$$

を *(i に付随する)* 超楕円的写像類群という.

(11) を mod 2 で還元して準同型

$$\overline{\psi}_* : \Gamma_g \longrightarrow \mathrm{Sp}(2g, \mathbb{F}_2) \tag{13}$$

が定まる.

命題 3 $i \in \Gamma_g$ を一つの超楕円対合とすると $\overline{\psi}_*(H_g(i)) \cong \mathcal{S}_n$.

証明. 以上はトポロジーの枠内の話であるから, 第 0 節のように $X(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ は 2 重被覆で $2g+2$ 個の分岐点集合 B は i の固定点集合と一致するとしてよい. このとき $\forall\, h \in H_g(i), P \in B$ に対して $ioh(P) = hoi(P) = h(P)$ よって $h(P) \in B$. よって $h \in H_g(i)$ は集合 B の置換 $\overline{h}$ を引き起こす. □

さて, X が k 上定義された代数曲線のとき, 外ガロア表現

$$\varphi_X : \mathrm{Gal}(\overline{k}/k) \longrightarrow \Gamma_g^{\mathrm{pro}-\ell} \tag{14}$$

が定まる. ここで $X = X_f/k$ が 超楕円曲線であれば k 上定義された超楕円対合 $i : (x, y) \mapsto (x, -y)$ が存在する. 従って, φ_X の像は $H_g(i)^{\mathrm{pro}-\ell}$ に含まれる. φ_{X_f} と ψ_* の pro-ℓ 版の合成が $\rho_{f,\ell}$ に他ならないから, これで $\overline{\rho}_{f,2}$ の像が 高々 $\mathcal{S}_{2g+2}$ であることの説明ができた.

4. 問題 2 とその反例

次に対応 $f(X) \to X_f$ がどのくらい "内在的" であるか, という素朴な疑問について簡単な考察をする. まず, $\overline{k}$ 上の同型に関しては Torelli の定理 によって

$$J_{f_1} \cong J_{f_2} \Leftrightarrow X_{f_1} \cong X_{f_2} \Leftrightarrow B_{f_1} = \gamma(B_{f_2}) \quad (\exists \gamma \in \mathrm{GL}(2, \overline{k}))$$

が成立することに注意する. そこで

• **問題 2** $f_1(X), f_2(X) \in k[X]$ に対して次の 2 条件がみたされるとき, J_{f_1}, J_{f_2} は $\overline{k}$ 上同種 (isogenous) であるか?

(i) f_1, f_2 の k 上の最小分解体は等しい: $\mathrm{Spl}(f_1/k) = \mathrm{Spl}(f_2/k)$
(ii) X_{f_1}, X_{f_2} の種数が等しい: $g(X_{f_1}) = g(X_{f_2})$

という問題を考える. k が有限体または代数体の場合は 同種定理 (Tate, Faltings) によって J_{f_1}, J_{f_2} が k 上同種であることと, 対応する ℓ-進ガロア表現が同値: $\rho_{f_1,\ell} \approx \rho_{f_2,\ell}$ であることは同値であるので, 条件 (i),(ii) から J_{f_1}, J_{f_2} が k 上同種であることは出ない. が, $\overline{k}$ で同種でない例を具体的にあげるのは (一般の体 k については特に) 難しいと思われる. ここで, 対応 $f \mapsto X_f$ についての Zarhin の一連の研究から次の結果を引用する:

定理 3 (Zarhin [11]) $f(X) \in k[X]$ は既約な $n(>4)$ 次式で, その k 上のガロア群が十分大きい (例えば $\mathrm{Gal}(f/k) = \mathcal{A}_n, \mathcal{S}_n$ の場合など) とする. このとき J_f は非自明な自己準同型をもたない, すなわち $\mathrm{End}_{\overline{k}}(J_f) \cong \mathbb{Z}$.

この定理を利用すると, 問題 2 に対する否定的な解をもつ例を与えることが出来る. 次の多項式族は Brumer の多項式族として知られているもの (と同値) である (a, b, c は独立なパラメータ).

$$\begin{aligned} f(a,b,c;X) \;:=\; & X^6 - (4+2b+3c)X^5 + (2+2b+b^2-ac)X^4 \\ & -(6+4a+6b-2b^2+5c+2ac)X^3 + (1+b^2-ac)X^2 + (2-2b)X + (1+c). \end{aligned} \tag{15}$$

この多項式族は次の著しい性質をもつ.

定理 4 $k = \mathbb{Q}(a,b,c)$ とおくと $\mathrm{Gal}(f(a,b,c;X)/k) = \mathcal{A}_5$ である.

実際, s, t, z を独立変数とする有理関数体 $\mathbb{Q}(s,t,z)$ の 2 個の $\mathbb{Q}$-同型を ψ, φ を

$$\psi : (s,t,z) \mapsto (t,z,s), \quad \varphi : (s,t,z) \mapsto (f(s,t,z),t,z),$$

$$\text{ただし} \qquad f(s,t,z) := \frac{-1+s+tz}{-1+st+sz+stz}$$

で定めるとこれらは 5 次交代群 $\mathcal{A}_5$ の良く知られた生成関係式

$$\varphi^2 = \psi^3 = (\varphi\circ\psi)^5 = 1$$

をみたす. 従って ψ, φ は 5 次交代群 $\mathcal{A}_5$ と同型な群 G を生成する. 一方, 関数 s の $G = \langle \psi, \varphi \rangle$ による軌道は 6 元集合

$$R(s,t,z) \;=\; \Big\{ s, t, z, f(s,t,z), f(s,t,z), f(s,t,z) \Big\} \tag{16}$$

であることが簡単な直接計算で示される. さらに次の事実も簡単に示される.

$$\begin{aligned} \mathrm{Aut}(R(s,t,z)) \;&:=\; \{\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(s,t,z)) \mid \sigma(R(s,t,z)) = R(s,t,z)\} \\ &=\; \langle \psi, \varphi \rangle \;=\; G. \end{aligned}$$

今 $R(s,t,z)$ の元を上記の順序に従って $x_1, \ldots, x_6$ と記すとき $\varphi = (14)(56), \psi = (123)(456), \varphi\circ\psi = (12346)$ と置換表現される. そして $f(a,b,c;X)$ は $R(s,t,z)$ を零点集合とする多項式を展開したものに他ならない:

$$f(a,b,c;X) \;=\; \prod_{x_i \in R(s,t,z)} (X - x_i). \tag{17}$$

さて, $f(a,b,c;X)$ のもう一つの著しい性質は, これに対応するヤコビ多様体 $X_f(a,b,c;X)$ が $\mathbb{Q}(\sqrt{5})$ の整数環を自己準同型環にもつことである:

定理 5 $\mathrm{End}_{\overline{k}}(J_{f(a,b,c;X)}) = \mathrm{End}_k(J_{f(a,b,c;X)}) \cong \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

この証明などの詳細については [1] を参照のこと. 今 $\{x_1, \ldots, x_6\} = R(s,t,z)$ から $\mathbb{Q}(s,t,z)$ に属する 5 個の元を

$$\begin{cases} y_1 = x_1x_2 + x_3x_6 + x_4x_5 \\ y_2 = x_1x_6 + x_2x_4 + x_3x_5 \\ y_3 = x_1x_5 + x_2x_6 + x_3x_4 \\ y_4 = x_1x_3 + x_2x_5 + x_4x_6 \\ y_5 = x_1x_4 + x_2x_3 + x_5x_6 \end{cases}$$

のように定める. このとき $R'(s,t,z) = \{y_1, \ldots, y_6\}$ は $G = \langle \psi, \varphi \rangle$ で全体として不変であり, $\{y_1, \ldots, y_5\}$ の置換としては $\psi = (12)(34)$, $\varphi = (154)$, $\varphi\circ\psi = (15342)$ となる. 特に $R'(s,t,z)$ を零点集合とする 5 次多項式の各係数は $\mathbb{Q}(s,t,z)^G = \mathbb{Q}(a,b,c) = k$ に属する:

$$g(a,b,c;X) := \prod_{i=1}^{5} (X - y_i) \quad \in \mathbb{Q}(a,b,c)[X] \tag{18}$$

そして $\mathbb{Q}(x_1, \ldots, x_6) = \mathbb{Q}(y_1, \ldots, y_6) = \mathbb{Q}(s,t,z)$ が容易に示される. すなわち $f_1(X) := f(a,b,c;X)$, $f_2(X) := f(a,b,c;X)$ の組は $k = \mathbb{Q}(a,b,c)$ に対して問題 2 の条件をみたす. 一方, $\deg(f_2) = 5$ で $\mathrm{Gal}(f_2/k) = \mathcal{A}_5$ であるから Zarhin [11] の定理によって $\mathrm{End}_{\overline{k}}(J_{f_2}) \cong \mathbb{Z}$. 従って J_{f_1}, J_{f_2} は $\overline{k}$ 上同種 (isogenous) とならない.

最後に, 等式 $\mathbb{Q}(s,t,z)^G = \mathbb{Q}(a,b,c) = k$ は 5 次交代群 $\mathcal{A}_5$ に対する前田氏の結果 [4](Noether の問題の肯定的解決) の, 3 次元 Cremona 変換群における類似であること, および同様な結果が 2 次元 Cremona 変換においても得られていること (c.f. [2]) を注意する. 特に後者を用いた前田氏の定理の別証明も得られている.

参考文献

[1] Hashimoto, K.: On Brumer's family of RM-curves of genus two, Tohoku Math. J. (2) **52** (2000), no. 4, 475–488.

[2] Hashimoto, K. and Tsunogai, H. : Generic Polynomials over Q with two parameters for the transitive groups of degree five , Proc. Japan. Acad. Vol.**79**. Ser.A.No 9 (2003), 142-145.

[3] Humbert, G : Sur les fonctions abéliennes singulières, Œuvres de G. Humbert **2**, pub. par les soins de Pierre Humbert et de Gaston Julia, Paris, Gauthier-Villars (1936), 297-401.

[4] Maeda, T. : Noether's Problem for A_5, J.of Algebra **125**(1989), 418-430.

[5] Meyer, W. : Signaturdefekte, Teichmüllergruppen und Hyperelliptische Faserungen, Hablitationsschrift, Universität Bonn, 1979.

[6] Milne, J.S. : Jacobian Varieties, in Arithmetic Geometry, ed. G.Cornell and J.H.Silverman, Springer-Verlag (1986), 167-212.

[7] Mori, S. : The endomorphism rings of some abelian varieties, Japanese J.Math. **2** (1976), 109-130; – II, ibid. **3** (1977), 105-109.

[8] Mumford, D. : Abelian Varieties, Oxford University Press: Oxford, 1970.

[9] Mumford, D. : Tata Lectures on Theta II, Birkhäuser, (1984).

[10] Serre, J-P. : Topics in Galois Theory, Research Notes in Mathematics **1**, Jones and Bartlett Publ. 1992.

[11] Zarhin, Yu.G. : Hyperelliptic jacobians without complex multiplication, Math. Res. Letters **7** (2000), 123-132.